

## 「DNS キャッシュポイズニング対策」の資料を公開

－DNS(Domain Name System)の役割と関連ツールの使い方－

IPA（独立行政法人情報処理推進機構、理事長：西垣 浩司）は、「DNS キャッシュポイズニングの脆弱性」の届出が多数継続していることから、これらの脆弱性対策を促進するため「DNS キャッシュポイズニング対策」の資料を2009年1月14日（水）より公開しました。

2008年7月にDNS(Domain Name System)<sup>1</sup>サーバ製品の開発ベンダーから「DNS キャッシュポイズニング（汚染）の脆弱性」の対策情報が公開されています<sup>2</sup>。この脆弱性を悪用した攻撃コードが公開されていたため、IPAはウェブサイト運営者へ向けて2008年7月24日に緊急対策情報を発表しました<sup>3</sup>。また、「実際に運用されているDNSサーバに対策が実施されていないのではないか？」という旨の届出<sup>4</sup>が激増したため、2008年9月18日<sup>5</sup>および2008年12月19日<sup>6</sup>に注意喚起を行いました。

今回公表した資料（全48ページ）は、「DNS キャッシュポイズニングの脆弱性」の対策を更に促進することを目的としており、DNS キャッシュポイズニング対策の検査ツールの使用方法や、DNSの適切な設定方法に関する情報等をまとめています。

第1章では、DNSの役割とその仕組み、DNS キャッシュポイズニングの実現手法とその脅威を解説しています。第2章では、DNSの問合せ動作を概説し、その動作の理解を深めて頂くための関連ツールとしてwhoisサービスやnslookupコマンドの使い方を説明しています。第3章では、DNS キャッシュポイズニング対策の検査ツールとして活用できるCross-Pollination Check ツールとDNS-OARC Randomness Test ツールの使い方と注意点をまとめてあります。第4章では、BIND DNSサーバとWindows DNSサーバの適切な設定に関して具体的に記述してあります。

本資料が、「DNS キャッシュポイズニングの脆弱性」対策の促進に寄与することを期待します。次のURLよりダウンロードの上、ご参照ください。

[http://www.ipa.go.jp/security/vuln/DNS\\_security.html](http://www.ipa.go.jp/security/vuln/DNS_security.html)

- 本件に関するお問い合わせ先  
IPA セキュリティセンター 山岸／渡辺  
Tel: 03-5978-7527 Fax: 03-5978-7518 E-mail: vuln-inq@ipa.go.jp
- 報道関係からのお問い合わせ先  
IPA 戦略企画部広報グループ 横山／大海  
Tel: 03-5978-7503 Fax: 03-5978-7510 E-mail: pr-inq@ipa.go.jp

<sup>1</sup> コンピュータがネットワークのどこに接続されているかを示すIPアドレスという数字の集まりを、www.ipa.go.jpのような人に覚えやすいドメイン表記と対応させるための情報を管理する仕組みです。

<sup>2</sup> 脆弱性対策情報データベース JVN iPedia「複数のDNS実装にキャッシュポイズニングの脆弱性」を参照ください。  
<http://jvndb.jvn.jp/ja/contents/2008/JVNDB-2008-001495.html>

<sup>3</sup> <http://www.ipa.go.jp/security/ciadr/vul/20080724-dns.html>

<sup>4</sup> ソフトウェア等の脆弱性関連情報に関する届出制度：経済産業省告示に基づき、2004年7月より開始しました。IPAは届出受付・分析、JPCERT/CCは国内の製品開発者などの関連組織との調整を行っています。

<sup>5</sup> [http://www.ipa.go.jp/security/vuln/documents/2008/200809\\_DNS.html](http://www.ipa.go.jp/security/vuln/documents/2008/200809_DNS.html)

<sup>6</sup> [http://www.ipa.go.jp/security/vuln/documents/2008/200812\\_DNS.html](http://www.ipa.go.jp/security/vuln/documents/2008/200812_DNS.html)